

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

CASE NO. 3:23-CV-395

UNITED STATES OF AMERICA

v.

ALL CRYPTOCURRENCY, VIRTUAL
CURRENCY, FUNDS, MONIES, AND OTHER
THINGS OF VALUE SEIZED, PURSUANT TO
A SEIZURE WARRANT, FROM BINANCE
AND ASSOCIATED WITH USER ID #
17392912, SUCH USER ID ASSOCIATED WITH
THE NAME, VIPIN KUMAR, AND TETHER
DEPOSIT ADDRESS,
TCJvnhLCvCwqEzcYiZKbr9F4pkkiLPGzyv; and

ALL CRYPTOCURRENCY, VIRTUAL
CURRENCY, FUNDS, MONIES, AND OTHER
THINGS OF VALUE SEIZED, PURSUANT TO
A SEIZURE WARRANT, FROM BINANCE
AND ASSOCIATED WITH USER ID #
159588534, SUCH USER ID ASSOCIATED
WITH THE NAME, RAHUL AGARWAL AND
TRON (TRX) DEPOSIT ADDRESS
TEp28dMpzcMo4X1rWb36gJ9HbWd1mqEtXS.

**COMPLAINT FOR
FORFEITURE *IN REM***

NOW COMES the United States of America, Plaintiff herein, by and through Dena J. King,
United States Attorney for the Western District of North Carolina, in a civil cause of forfeiture,
and respectfully states the following:

INTRODUCTION

1. This action seeks the forfeiture of cryptocurrency derived by one or more unidentified members of an unidentified criminal group (“UCG”) who conducted a “Crypto Website Spoofing Scheme”—that is, a scheme wherein the members of the UCG fraudulently used a spoofed cryptocurrency exchanger website and other means to fraudulently identify themselves as customer service representatives of a legitimate cryptocurrency exchanger. When victims

accessed the spoofed website, which appeared to be the legitimate cryptocurrency exchanger's website but was not, in actuality, affiliated in any way with the legitimate cryptocurrency exchanger, the UCG created a façade that the victims' accounts at the legitimate cryptocurrency exchanger were locked. Thereafter, the UCG falsely purported to be representatives of the legitimate exchanger and offered assistance in unlocking victims' accounts which, of course, in reality, were not locked and only appeared so on the spoofed website. Through the UCG's misrepresentation to victims that the UCG would assist in unlocking accounts, the UCG induced victims to provide sensitive personal information, such as user names and passwords, and copies of identification documents, to members of the UCG. Thereafter, the UCG used the sensitive personal information to access, without authorization, victim accounts, including accounts of victims in the Western District of North Carolina. In this manner, the UCG drained victims' accounts of assets. Then, the UCG conducted myriad transactions in proceeds, layering the transactions through multiple accounts and funneling proceeds into and out of accounts in an attempt to obfuscate the origins of the proceeds and make tracking the proceeds all the more difficult. Via this scheme, the UCG obtained the CRYPTOCURRENCY identified for seizure herein that, until law enforcement execution of Seizure Warrants, was held in the TARGET ACCOUNTS identified below.

2. Specifically, this action seeks the forfeiture of seized cryptocurrencies, virtual currency, funds, monies, and other things of value (hereafter, "cryptocurrency," "Ether," "Tether," and "Polkadot") previously stored in or accessible at Binance Holdings Ltd d.b.a. "Binance" (which owns and operates the Binance cryptocurrency exchange) and associated with the following User IDs, conspirators, and addresses:

- a. User ID # 17392912, suspected conspirator Vipin Kumar, and Tron (TRX) Deposit address, TCJvnhLCvCwqEzcYiZKbr9F4pkkiLPGzyv (hereafter,

“TARGET ACCOUNT A”). At the time of seizure by law enforcement, the contents of TARGET ACCOUNT A consisted of at least approximately 3,400,000 Tether (“USDT”) and 100 Ether (ETH); and 71012.46 Polkadot (DOT); and

b. User ID # 159588534, suspected conspirator Rahul Agarwal and Tron (TRX) deposit address TEp28dMpzcMo4X1rWb36gJ9HbWd1mqEtXS, (hereafter, “TARGET ACCOUNT B”). At the time of seizure by law enforcement, the contents of TARGET ACCOUNT B consisted of at least approximately 21,257 Tether (“USDT”),

(collectively, “the CRYPTOCURRENCY” and “the TARGET ACCOUNTS”).

3. The CRYPTOCURRENCY constitutes or is derived from proceeds of wire fraud conspiracy and wire fraud in violation of 18 U.S.C. §§ 1343 and 1349, and property involved in money laundering and money laundering conspiracy in violation of 18 U.S.C. §§ 1956, 1956(h), and 1957.

JURISDICTION AND VENUE

4. This is a civil action *in rem* pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C). Procedures for this action are mandated by Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981, 983, and 984, and the Federal Rules of Civil Procedure.

5. This Court has jurisdiction over this action commenced by the United States under 28 U.S.C. § 1345 and over this action for forfeiture under 28 U.S.C. § 1355(a). The Court has in rem jurisdiction over the defendant property under 28 U.S.C. § 1355(b).

6. This Court has venue pursuant to 28 U.S.C. §§ 1355 and 1395. Venue is proper because the acts or omissions giving rise to the forfeiture occurred in this district, the claim accrued in this district, and the CRYPTOCURRENCY was found in this district.

7. Specifically, in or about December of 2022, the United States Secret Service (“USSS”), served federal Seizure Warrants for forfeiture of the CRYPTOCURRENCY. The USSS in the Western District of North Carolina is currently holding the CRYPTOCURRENCY.

8. Pursuant to Supplemental Rule G(2)(f), facts in support of a reasonable belief that the Government will be able to meet its burden of proof at trial are set forth more fully as follows and have been verified by the attached Verification of USSS Special Agent Christopher Maier.

DEFINITIONS

Virtual Currency Exchangers

9. At the times set forth herein, virtual currency “exchangers” and “exchanges” were individuals or companies that exchanged virtual currency for other currencies, including U.S. dollars.

10. For example, at the times set forth herein, Binance and another entity identified herein as “Legitimate Exchanger” were full-service cryptocurrency exchangers and offered services to account holders.

Binance

11. Binance facilitated the purchase, sale, and transfer of a variety of digital currencies. Binance identified accounts using a variety of target identifiers, including the identifiers provided herein for the TARGET ACCOUNTS.

Legitimate Exchanger

12. At the times set forth herein, Legitimate Exchanger, the publicly traded exchanger that serves legitimate purposes, maintained a legitimate website (“the Legitimate Exchanger Website”).

13. At the times set forth herein, Legitimate Exchanger was an advanced trading platform advertised for Legitimate Exchanger's customers who frequently trade cryptocurrency. According to the Legitimate Exchanger Website, users of cryptocurrency (users such as the victims identified herein), would access the Legitimate Exchanger Website and services to buy, sell, and manage cryptocurrency.

14. The Legitimate Exchanger Website is not the same as the Phishing Exchanger Website that the UCG used, as described below.

THE SPOOFING SCHEME

15. Beginning no later than January 2022, the UCG used what is described herein as a Phishing Exchanger Website to conduct their scheme and obtain assets, including the CRYPTOCURRENCY identified herein, from victims.

16. Specifically, the Phishing Exchanger Website could be found at different variations of internet addresses similar to the address of the Legitimate Exchanger Website.

17. The UCG used these variations on the Legitimate Exchanger Website to redirect unsuspecting victims—victims who were searching for the Legitimate Exchanger Website, and Legitimate Exchanger services—to fraudulently created phishing websites, that is, websites designed by conspirators to mimic the appearance of legitimate websites, falsely gain the trust of users, and fraudulently obtain users' personal and private information, including sensitive account information.

18. Specifically, often, when users conducted a web search from their web browser on a device, whether that search be via Safari (Apple based devices), Google, or Edge, in an attempt to access the Legitimate Exchanger Website, instead of being directed to the Legitimate Exchanger Website, there was a redirect of the victim's initial search to a Phishing Exchanger Website.

19. For example, when searching for the Legitimate Exchanger Website, one victim inadvertently typed in a Phishing Exchanger Website address. This search revealed a well-constructed webpage, similar in appearance to the Legitimate Exchanger Website, with high-quality graphics and login screen that prompted the user to provide the user's username and password, a prompt consistent with the Legitimate Exchanger Website.

20. However, notwithstanding the compelling appearance of the Phishing Exchanger Website, most icons and links featured on the webpage were inoperable via a desktop computer. The webpage was essentially a single page without functioning links. Some links would only display an "account is disabled"-type pop up screen regardless of the context of the link. The website also featured several instances of improper terminology and grammatical errors, such as words lacking proper capitalization or structure. This website that included improper terminology and grammatical errors is not indicative of a website operated by an organized, publicly traded company such as the Legitimate Exchanger. Further, when these websites were accessed, numerous redirections and misdirections occurred, with one or more members of the UCG constantly posing as customer service representatives and requesting sensitive information.

21. No matter what a user entered on the Phishing Exchanger Website, the phishing website indicated that the user's account was disabled or locked and that assistance from a customer service representative was required. Through these interactions between users and purported customer service representatives, the UCG obtained and, ultimately, exploited, sensitive personal information, such as account information and identifying documents, from users.

22. Each of the victims identified herein accessed a spoofed Phishing Exchanger Website, like the websites described herein, and somehow provided access to or information about

the victim's cryptocurrency account such that the UCG was able to access the victims' cryptocurrency and launder it through multiple accounts.

THE UCG DEFRAUDS VICTIMS, GAINS ACCESS TO THEIR ACCOUNTS, USES THAT ACCESS TO FUND THE TARGET ACCOUNTS, AND LAUNDERS THE ASSETS VIA A COMPLEX FUNNELING AND LAYERING SCHEME

Overview

23. After the UCG used a spoofed Phishing Exchanger Website to obtain information about victims, including victims in the Western District of North Carolina, and access victims' assets, the UCG moved assets obtained from victims to and through TARGET ACCOUNT A and TARGET ACCOUNT B, as well as to and through myriad other accounts. Below are only a few sample transactions out of myriad transactions identified to-date.

VICTIM ONE

24. At the times set forth herein, VICTIM ONE was a resident of California.

25. On January 25, 2022, VICTIM ONE attempted to access his Legitimate Exchanger account but typed an address that was not the address for the Legitimate Exchanger Website. The address routed VICTIM ONE to a Phishing Exchanger Website. At that point, a message appeared on the top of the website that said that VICTIM ONE's account was locked and to call a number and/or use the live chat function. VICTIM ONE gave the UCG the two-factor number from the victim's phone to access to the account. VICTIM ONE reports that VICTIM ONE was unaware that providing such information to the UCG would give total access to the victim's account and assets held at Legitimate Exchanger.

26. After VICTIM ONE had given access to the account, 70.63 Ether was subsequently transferred out of VICTIM ONE's Legitimate Exchanger wallet, via two transfers to the UCG at the wallet 0x00f02, and then to multiple decentralized cryptocurrency wallets under the control of

the UCG. Ultimately, this 70.63 in Ether derived from VICTIM ONE was moved and converted/exchanged to USDT (other victim assets were converted/exchanged in a similar manner), commingled with other victim assets, and placed in TARGET ACCOUNT A at the Binance cryptocurrency exchange.

VICTIM TWO

27. At the times set forth herein, VICTIM TWO was a resident of the Western District of North Carolina.

28. On April 16, 2022, VICTIM TWO attempted to access VICTIM TWO's Legitimate Exchanger account, but a Phishing Exchanger Website similar or identical to the Legitimate Exchanger Website appeared to VICTIM TWO. VICTIM TWO entered the victim's account ID and password on the website. The website refreshed with a new screen that indicated that VICTIM TWO's account was locked and to call a number or communicate with what the victim believed was Legitimate Exchanger's customer service via a pop-up screen. Unbeknownst to VICTIM TWO, the purported customer service representative was a UCG imposter posing to be affiliated with Legitimate Exchanger. UCG convinced VICTIM TWO to provide access to the account.

29. After VICTIM TWO provided a two-factor authorization password, VICTIM TWO was told that the account was fixed and to access it. VICTIM TWO realized the website was not legitimate, accessed the account, and saw \$132,515.51 in U.S. Currency in the account for a few moments. At this time, VICTIM TWO received emails that transactions were taking place without the consent of VICTIM TWO. VICTIM TWO noticed the \$132,515.51 was exchanged for Ether but also received notifications the UCG attempted to exchange the Ether for USDT but that the exchange was cancelled.

30. After VICTIM TWO had given access to the account, 43.60 Ether was transferred out of VICTIM TWO's Legitimate Exchanger wallet to multiple decentralized service cryptocurrency wallets under the control of the UCG at 0xbd85f4. Furthermore, 8.81 Ether was consolidated from two other victims and consolidated into VICTIM TWO's transfer for a total of 52.90 Ether. Ultimately, at least 52.90 Ether of VICTIM TWO was exchanged, commingled, and funded TARGET ACCOUNT A at the Binance cryptocurrency exchange.

VICTIM THREE

31. At the times set forth herein, VICTIM THREE was a resident of Florida.

32. On June 6, 2022, VICTIM THREE attempted to enter the Legitimate Exchanger Website but typed an address that was not the address for the Legitimate Exchanger Website into the victim's web browser. The browser revealed a site that appeared identical to the Legitimate Exchanger Website but was, in fact, a Phishing Exchanger Website. VICTIM THREE entered the victim's username and password, which initiated a banner along the top of the webpage. The banner indicated there was a security issue and to call a particular phone number. VICTIM THREE called the number provided, wherein a UCG operator claimed to be a Legitimate Exchanger representative for high value accounts and indicated that he could help VICTIM THREE navigate an account reset while waiting on the phone. VICTIM THREE was instructed to click the chat icon on the bottom right corner of the screen. Later in the chat, VICTIM THREE was asked to provide the UCG with authentication codes that had been sent to VICTIM THREE's phone. VICTIM THREE provided the codes.

33. Once the UCG had account information and authentication codes from VICTIM THREE, the UCG used this two-factor authentication code to access VICTIM THREE's Legitimate Exchanger account. VICTIM THREE also uploaded copies of the victim's Driver's

License to the web chat, as instructed by UCG. Later, after checking the account, VICTIM THREE realized that the UCG had exchanged all of VICTIM THREE's Loop Ring Token (LRC) to Ether (ETH), and then, after bypassing account verification with the ID, transferred the Ether out of the account.

34. Ultimately, after VICTIM THREE had given access to the account, \$287,323.00 in US Currency was exchanged for 178.56 Ether and was subsequently transferred out of VICTIM THREE's Legitimate Exchanger wallet to multiple decentralized service cryptocurrency wallets under the control of UCG at 0x484283. At least 49,960 USDT of VICTIM THREE's 178.56 Ether funded TARGET ACCOUNT B at the Binance cryptocurrency exchange and, through a series of convoluted and complex transactions, also funded transactions to other locations.

Total Fraud Identified To-Date

35. In summary, the UCG defrauded the specific victims herein of at least 322.99 Ether (ETH) and 0.955337 Bitcoin (BTC), which were collectively worth approximately \$779,374.87 in U.S. Currency at the time of the transactions. The UCG also defrauded other victims that funded the TARGET ACCOUNTS and other accounts. To-date, law enforcement has specifically traced the involvement of the TARGET ACCOUNTS to the fraud on the specific victims described herein and has linked numerous other victims and at least \$9 million in victim losses to the UCG's Phishing Exchanger Website scheme more generally.

36. The TARGET ACCOUNTS did not have any legitimate purpose or obtain funding from legitimate sources. Instead, the TARGET ACCOUNTS existed to facilitate transactions in assets unlawfully obtained from victims.

USSS SEIZES THE CRYPTOCURRENCY

37. In or about December of 2022 through early 2023, USSS obtained and executed Seizure Warrants for the contents the TARGET ACCOUNTS and ultimately seized the CRYPTOCURRENCY.

CONCLUSION

38. By virtue of the foregoing and pursuant to 18 U.S.C. § 981(b), all right, title, and interest in the CRYPTOCURRENCY vested in the United States at the time of the commission of the unlawful act giving rise to forfeiture and has become and is forfeitable to the United States.

WHEREFORE, the United States of America respectfully prays the Court that:

1. Due notice be given to all parties to appear and show cause why the forfeiture should not be decreed;
2. Judgment be entered declaring the CRYPTOCURRENCY to be condemned and forfeited to the United States of America for disposition according to law; and
3. The United States be granted such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action, including but not limited to the expenses of maintenance and protection of the CRYPTOCURRENCY as required by 28 U.S.C. § 1921.

Respectfully submitted, this the 30th day of June, 2023.

DENA J. KING
UNITED STATES ATTORNEY

s/Benjamin Bain-Creed
FL Bar Number 21436
Assistant United States Attorney
Suite 1650, Carillon Building

227 West Trade Street
Charlotte, North Carolina 28202
Telephone: (704) 344-6222
Facsimile: (704) 344-6629
Email: benjamin.bain-creed@usdoj.gov

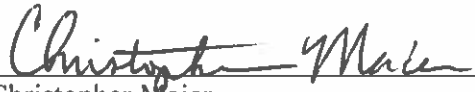
STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG

VERIFICATION

Christopher Maier deposes and says under penalty of perjury:

I am a Special Agent with the United States Secret Service and one of the agents assigned to this case.

I have read the foregoing Complaint and the factual information contained therein is true according to the best of my knowledge, information, and belief.



Christopher Maier
Special Agent
United States Secret Service